第1章

あなたが設計したLSIから秘密情報が漏れてます

―― 暗号回路のトレンドはアルゴリズムの標準化から実装の安全性評価へ

佐藤 証

LSIからのデータの読み出しは，I/Oポートを介してのみ行われるわけではない．LSIが演算を行っているときに発する電磁波や熱，音などを測定，解析して，データを読み取ることもできる（いわゆる，サイドチャネル攻撃）．例えば，暗号回路部の処理を解析して秘密かぎを割り出されると，企業秘密や個人情報が読み取られてしまう可能性がある．ここでは，暗号技術の歴史を交えながら，サイドチャネル攻撃についての業界の動向を紹介する．　（編集部）

非接触ICカードやRFIDタグといった小型デバイスを用いた無線通信技術が，身近な生活の中にどんどん広がっています．非接触型のICカード方式に対応した自動改札や携帯電話が増えていますし，2005年日本国際博覧会（通称「愛・地球博」）の入場券にRFIDタグが使われたのも記憶に新しいと思います．キャッシュ・カードやクレジット・カードについても，偽造対策のため，接触型ICカードへの移行が進んでいます（右掲のコラム「ICカードのセキュリティ」を参照）．以前は，磁気ストライプに数十バイトのデータが書き込まれていただけでした．

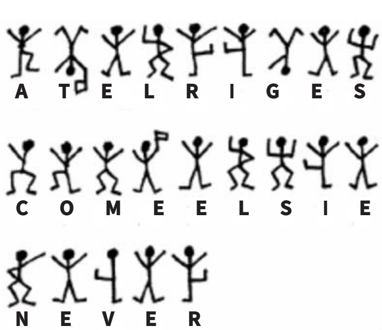


図1　シャーロック・ホームズの踊る人形

文字と人形が1対1に対応している．ホームズは人形の出現頻度の偏りを利用して解読に成功した．

● I/Oピンからでなくてもチップの情報は読みとれる

RFIDや非接触型ICカードの情報のやり取りが電波を通じて行われるように，LSIチップのデータ入出力はI/Oポートの電流・電圧変化を用いて行われます．しかしこれ以外にも，チップ全体の消費電力，配線からの電磁放射，そして熱，音，光など，さまざまな経路を通じて，チップ内部の情報は外部に漏れているのです．このような本来のデータの入出力経路（チャネル）ではないものを利用して，機密情報，とくに暗号化の秘密かぎなどを取り出そうとするのが「サイドチャネル攻撃」です．

2000年前後は暗号アルゴリズムの標準化がセキュリティ業界の大きな話題でした．ここ数年は，暗号モジュールの実装評価についての標準化活動が活発で，その中でもサイドチャネル攻撃とその防御法に関する研究が注目されています．まずは，このような暗号業界の流れを見ていきましょう．

1 暗号アルゴリズムの歴史と標準化

人類が文字を発明して以来，数限りない暗号が考案されています．シャーロック・ホームズの「踊る人形」[1]は有名ですし，古代エジプト文字「ヒエログリフ」も考古学者や言語学者以外の人たちにはある種の暗号といえるでしょう（**図1**）．ですが，踊る人形はちょっとした規則さえわかればだれでも読み書きできますし，ヒエログリフも当時の人にとっては暗号ではありませんでした．

● 現代暗号は「アルゴリズム」と「かぎ」が分離

これらに対して，現代暗号と呼ばれるものは次の2点が大きく異なります．

◉COLUMN◉ ICカードのセキュリティ

接触型ICカードであれば，どれが通信するべき端末なのかがその場でわかります．一方，非接触型ICカードの場合，だれかが盗み聞きしているかもしれません．RFIDは数十～数百ビットの認識番号（ID）を周りに伝えるだけなので，それほど問題にはなりませんが，かりにキャッシュ・カードやクレジット・カードだったらどうでしょう．影で第三者が成りすましの通信を行っているかもしれないという不安を持つと思います．ですが，キャッシュ・カードやクレジット・カードに用いるような高機能のICカードでは，機密データの暗号化と通信相手の正当性の検証がしっかりと行われているので，接触・非接触にかかわらずそのような心配はありません．

以前，テレビの報道番組でICカード情報をコートの上から読み取る「非接触スキミング」という光景を目にしたことがあります．ですが，初めに相手を確認し，また自分がだれかを知らせなければ通信は始められないので，そのようなID情報は読めてあたりまえなのです．このことと，セキュリティ機能を持たず，すべてのデータが簡単にコピーできる磁気カードのスキミングを同等に扱うのは誤りです．

ICカードのデータは，暗号アルゴリズムだけで守られているわけではありません．物理的な攻撃への対策として，多くのカードは電圧，周波数，光，温度などに対するさまざまなセンサを搭載しています．また，こうしたICカードのカタログには，"simple power analysis（SPA）"，"differential power analysis（DPA）"，"differential fault analysis（DFA）"，"electromagnetic analysis（EMA）"など，不当な方法による情報漏えい（いわゆるサイドチャネル攻撃）の対策についての記載があります．

- アルゴリズムとかぎが分かれている
- アルゴリズムを公開できる

かぎそのものがアルゴリズムの一部となってしまっている昔の暗号は，すべてを秘密にする必要がありました．現代暗号では，アルゴリズムとかぎを分けたことで，公の場でアルゴリズムに関する議論が可能となりました（ただし，特殊用途ではアルゴリズムが公開されていないものもある）．

本誌2004年12月号の表紙を飾ったEnigma（エニグマ）暗号機をご存じの方も少なくないと思います（**写真1**）．ドイツ軍が第2次世界大戦中に使用した機械式暗号機の傑作で，現在でもオークションで100万～300万円ほどの値段で取り引きされています．その原理は，キーを叩くたびに，入出力の配線がランダムにつながれた複数のロータが回転し，文字の変換規則を次々に変えていくというものです（p.102のコラム「Enigma暗号機」を参照）．

Enigma暗号機では，ロータの種類や順番，初期位置などが秘密かぎとなりますが，暗号機の構造（つまりアルゴリズムそのもの）も解析に非常に重要な手がかりを与えてしまいます．この点で，現代暗号とはいえません．



写真1 Enigma暗号機 提供：©Science & Society Picture Library

● 共通かぎ暗号のDESと公開かぎ暗号のRSA

Alan Turing（1912年～1954年）率いる英国の暗号解読チームは，さまざまな手がかりと数学・言語学などの知識を駆使して，Enigmaをはじめとするドイツ軍の暗号を次々と破っていました．また，彼らは暗号解読のために世界初のコンピュータ「Colossus（コロッサス）」を製作しています．

第2次世界大戦後しばらくは，軍事用の武器に相当するとして，暗号の使用に強い制限が課せられていました．それからしだいに規制が緩和され，今では業務から日常生活まで，用途に応じてさまざまな暗号アルゴリズムが利用されています．その中で，とくに有名なアルゴリズムとして，DES（Data Encryption Standard）とRSAが挙げられます．DESは，1977年に米国の連邦標準として制定され，現在，暗号製品の8割以上に実装されていると言われています．また，RSAはDESと同じ年に米国Massachusetts Institute of Technology（MIT）のRivest，Shamir，Adlemanらによって開発されました．RSAは彼らの頭文字を取って名づけられました．この3人はその功績が認められ，2002年にコンピュータ・サイエンスのノーベル賞と称されるチュー

リング賞を受賞しています．

DESは共通かぎ暗号で，高速なデータ処理を行います．共通かぎ暗号は，暗号化と復号に同じかぎを用いる方式です．一方，RSAは公開かぎ暗号に属します．これは，暗号化に「公開かぎ」，復号に「秘密かぎ」という二つの異なるかぎを使用します．公開かぎ暗号はデータ処理が低速ですが，その反面，共通かぎ暗号では対応できないかぎ交換やディジタル署名などに利用できます．

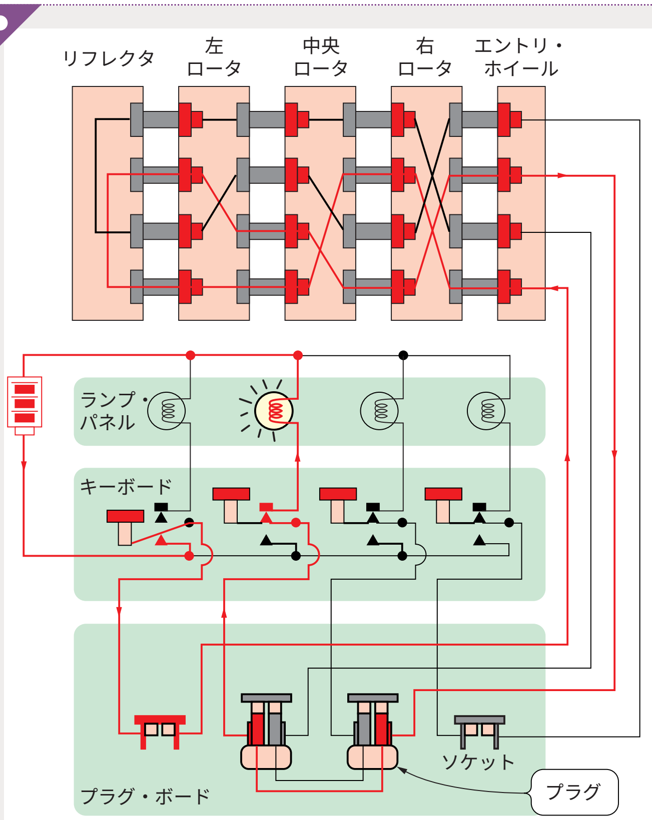
● コンピュータの性能向上に伴い，解読技術も進化する

DESとRSAが開発されてからすでに30年になろうとしています．その間，飛躍的に向上したコンピュータの性能と，急速に拡大するネットワークを活用した分散処理は，暗号アルゴリズムの安全性の大きな脅威となっています．

RSA暗号はかぎの長さが可変であり，512ビット，1,024ビット，2,048ビットと拡張することで，まだまだ現役の地位を保っています．これに対して，DESはかぎの長さが56ビット固定であるため，今では2^{56}個のかぎをすべて試すという方法を採っても，解読に1日かかりません．もちろん，米国標準技術研究所（NIST：National Institute of Standards and Technology）は，このような状況を静観していたわけではありません．56ビットのかぎを二つ，または三つ用いてDESの処理を3回繰り返す「Triple-DES」という規格を1997年に暫定的な標準として制定しています．

それと同時に次世代の共通かぎ暗号標準を決めるAES（Advanced Encryption Standard）プロジェクトを立ち上げ，世界中からアルゴリズムを公募しました．3回の国際会議を経て，ベルギーから提案されたアルゴリズム（Rijndael）をAESとして採用しました．AESのかぎ長は，128，192，256ビットの中からいずれかを選択します．

AESプロジェクトを発端として，欧州のNESSIE（New European Schemes for Signature, Integrity, and Encryption），日本国内のCRYPTREC（Cryptographic Research and Evaluation Committee），そしてISO（International Organization for Standardization）において，暗号アルゴリズムの評価・標準化作業が活発に繰り広げられました．暗号アルゴリズムの標準化活動はひと段落した感がありますが，国内外の学会では引き続き，暗号の



図A-1　Enigma暗号機の動作原理

◉COLUMN◉　Enigma暗号機

Enigma暗号機にはいくつかのバリエーションが存在します．例えば，本文の**写真1**で紹介したものは，上部に三つのロータを持つタイプです．

図A-1はEnigma暗号機の動作原理を簡単に示したものです．ロータの下は暗号化された文字が点灯するランプ・パネル，その下が平文を入力するキーボード，そしていちばん下が文字の入れ替えを行うプラグ・ボードです．キーを押すと，プラグ・ボード，ロータ，ランプ・パネル，内蔵バッテリを結ぶ閉回路ができて，選ばれたランプが一つだけ点灯するしくみになっています．

このEnigma暗号機の基本ロータは5種類で，その両側には26個の金属の接点があり，内部で入出力をランダムにねじるような配線が施されています．各ロータの周りにはアルファベット26文字が記された調節リングがはめられ，暗号機本体にセットしたときにその文字の一つが初期位置として小窓から現れます．右端のロータは文字を入力するごとに一つ位置がずれ（回転し）ます．中央のロータは26文字入力ごとに一つ，左端のロータは26×26＝676文字入力ごとに一つ回転します．このロータの種類や位置の組み合わせが無数にあるため，ドイツ軍は解読不可能と考えていました．そこで，ドイツ語で「なぞ」を意味する「Enigma」という名まえが付けられました．

解析や攻撃法，効率的で安全な実装，アプリケーションなど，幅広いテーマに大勢の研究者が取り組んでいます．

2 セキュリティ製品の評価制度

多数の研究者によって公開の場で評価された標準暗号を使うかぎり，アルゴリズムそのものの欠陥によって秘密かぎが漏れてしまう，といった心配は不要でしょう．しかし，実装や運用による不備がもとで，秘密かぎが盗まれてしまうことは十分に考えられます．例えば，秘密かぎをUSBメモリにそのまま入れているシステムが多く存在します．また，パスワードをメモ書きしてパソコンのディスプレイに貼っておくという人も多いでしょう．

もちろん，なんでもかんでもガチガチに管理すればよいというものではありません．守るべきものへの費用対効果や利便性などを考慮して，適切な製品や管理方法などを選択すればよいのです．とはいえ，すべてのユーザが暗号や情報セキュリティに詳しいわけではないので，安全なのかそうでないのかを自分自身で判断できないこともあります．また，メーカが「セキュリティは万全です」と言ったとしても，つねに信用できるとは限りません．

● 暗号モジュールのセキュリティ評価基準も標準化へ

そこで登場するのが，情報セキュリティ製品の国際評価基準「ISO/IEC 15408 Common Criteria」です（**図2（a）**）．これは，製品開発者がセキュリティ目標を定め，それが正しく実装され，想定した環境において矛盾なく動作することを公的な第三者機関が検証することを規定したものです．ICカードのカタログには，「ISO/IEC 15408 EAL4」といった表記が見受けられます．このEALは"Evaluation Assurance Level"の略で，1～7のレベルが設定されています．レベルの高いものほど，セキュリティ目標に記載された事項がより厳密に検証されていることを表しています．

ただし，セキュリティ目標は開発者が自由に定めることができるので，製造から配送までの間に製品に改変が加えられていないことを保障する場合もあれば，暗号機能を対象外とする場合もあるなど，千差万別です．EALのレベルがセキュリティ強度を示すものではないことに注意が必要です．

ISO/IEC 15408を取得する製品が増えるにしたがって，製品カテゴリに応じた標準的なプロファイルが順次でき上がっています．こうした中，高いレベルのEALを取得するということは，セキュリティに真剣に取り組んでいる姿勢の表れでしょう．日本政府もISO/IEC 15408を取得した製品の利用を推進しています．

ISO/IEC 15408はセキュリティ製品全般に対する評価基準であるのに対して，FIPS 140-2はNISTが定めたソフトウェア，ハードウェア，ファームウェアを含む暗号モジュールに限定した評価基準です（**図2（b）**）．これは米国内の標準ですが，多くの製品がこの認証を取得しており，2005年中にはISO/IEC 19790として国際標準化される予定です．暗号モジュールに課せられるセキュリティ要求事項は，**表1**に示すように11項目に分けて定められており，各項目がどれだけきちんと満たされているかによって1～4にレベル付けされます．例えば，**表1**の項目7で定められた安全な場所（ハードウェア）に秘密かぎを保管しないソフトウェアは，どんなにがんばってもレベル1しか取得できません．

現在，FIPS 140-2でとくに問題になっているのは，項目11の「そのほかの攻撃への対処」に分類されるサイドチャネル攻撃です．NISTはこれらに関する最新の研究を取り入れて要件を定め，2006年に改訂版FIPS 140-3を標準化することを予定しています．

● 国内でもサイドチャネル攻撃の研究が盛んに

サイドチャネル攻撃とその防御法に関する研究は，情報セキュリティ製品（とくにICカード）を開発・製造している企業が力を入れています．アルゴリズム・レベルの論理的な対策に関する論文は多数発表されているのですが，物理的な実装ノウハウが公開されることはほとんどありませ

（a）ISO/IEC15408 Common Criteria　（b）FIPS140-2

図2　製品のセキュリティを認証する

（a）はISO/IEC 15408 Common Criteriaの国際相互認証マークであり，Common Criteriaの頭文字と地球儀がモチーフになっている．国内ではJEITA（電子情報技術産業協会），ECSEC（電子商取引安全技術研究組合），みずほ総合研究所の三つの評価機関があり，その評価レポートを受けてIPA（独立行政法人 情報処理推進機構）が認証を行う．（b）は，FIPS140-2の認証マーク．米国とカナダが共同運用している評価制度CMVP（Cryptographic Module Validation Program）によって発行されるので，両国の国旗がデザインに取り入れられている．

表1
FIPS140-2のセキュリティ要求事項
暗号モジュールに対して定められたセキュリティ要求事項のそれぞれに対して，レベル1〜4の評価が与えられる．

	セキュリティ要求事項	規定内容
1	暗号モジュール仕様	暗号モジュールの仕様とセキュリティ・ポリシ
2	暗号モジュールのポート・インターフェース	データに応じたインターフェースの規定
3	役割，サービス，および認証	オペレータごとの役割とサービスの提供，オペレータの認証
4	有限状態モデル	状態遷移図による動作の規定
5	物理セキュリティ	皮膜，カバー，タンパ応答回路などの物理的セキュリティ
6	動作環境	動作環境および管理
7	暗号かぎ管理	乱数およびかぎ生成，保管，入出力など
8	電磁妨害，電磁両立性（EMI/EMC）	米国連邦通信委員会（FCC）要求事項の準拠
9	自己テスト	暗号アルゴリズムや完全性などのテストとエラー時の規定
10	設計保証	構成管理，配付および運用，開発，ガイダンス文書の規定
11	そのほかの攻撃への対処	FIPS140-2で規定されていないサイドチャネル攻撃対策など

ん．また，攻撃についても実際のセキュリティ製品を対象とするには大きな問題があります．

そこで第三者的な立場から，実装アルゴリズムの評価とノウハウの蓄積を行おうという取り組みが国内でも始まっています．CRYPTRECは，暗号モジュール委員会を設置し，評価・試験基準の検討を行っています(2)．また，日本規格協会の情報標準化研究センター（INSTAC：Information Technology Research and Standardization Center）からは，CPU（Z80およびPowerPC）ボード上のDESのサイドチャネル攻撃に関する研究報告書(3), (4)が公開されています．さらに，INSTACは，CRYPTRECでサイドチャネル攻撃の評価用標準プラットホームとして使用するFPGAボード（米国Xilinx社製「Virtex-II」を搭載）も開発しており，今後これらを用いたAESやRSAに対する実装攻撃・防御の評価が予定されています．

参考・引用*文献

(1) コナン・ドイル（山中 峯太郎 訳）；踊る人形，ポプラ社，1976年．
(2) 独立行政法人 情報処理推進機構，独立行政法人 情報通信研究機構；CRYPTREC Report 2004 暗号モジュール委員会報告書，2005年（平成17年）3月，http://www.ipa.go.jp/security/enc/CRYPTREC/fy16/documents/C04mod.pdf.
(3) 財団法人 日本規格協会；耐タンパー性に関する標準化調査研究開発報告書，2004年（平成16年）3月，http://www.jsa.or.jp/domestic/instac/committe/H15report/mokuji.htm.
(4) 財団法人 日本規格協会；耐タンパー性に関する標準化調査研究開発報告書，2005年（平成17年）3月，http://www.jsa.or.jp/domestic/instac/syoukai/H16/01_06.pdf.

さとう・あかし
日本アイ・ビー・エム（株）東京基礎研究所

◉COLUMN◉　暗号とデータ圧縮

英文では文字EやTの出現頻度がとくに高く，XやZはほとんど現れません．また，Qにはほとんどの場合Uが続くというように，文章中の文字列パターンには統計的な偏りがあります．シャーロック・ホームズの踊る人形は，アルファベットと人形が1対1に対応する暗号で，元の文章の統計的性質をそのまま保持していたため，すぐに解読されてしまったのです．このような統計的な偏りをなくすことが，現代暗号には最低限求められます．

ところで，通信文の統計的性質をうまく利用したアプリケーションに「モールス信号」があります．**表B-1**のように頻繁に現れる文字には短い符号語を，使用頻度の低い文字には長い符号語を割り当てて，通信時間を短縮します．データ圧縮の草分けとも言えます．

今日では，用途に応じてさまざまなデータ圧縮アルゴリズムが開発されていますが，それらはすべてモールス信号のようにデータの統計的性質をうまく利用しています．ですから，統計的性質が隠ぺいされた暗号文を圧縮することはできません．データの暗号化と圧縮を行いたいときには，かならず圧縮を先に行う必要があります．

余談になりますが，モールス信号の“SOS”は何かの略語ではなく，だれが聞いてもすぐに緊急事態であることがわかるように，特徴的なパターン“・・・ ― ― ― ・・・”が選ばれたのです．

表B-1　モールス信号

A	・―	J	・― ― ―	S	・・・
B	―・・・	K	―・―	T	―
C	―・―・	L	・―・・	U	・・―
D	―・・	M	― ―	V	・・・―
E	・	N	―・	W	・― ―
F	・・―・	O	― ― ―	X	―・・―
G	― ―・	P	・― ―・	Y	―・― ―
H	・・・・	Q	― ―・―	Z	― ―・・
I	・・	R	・―・		